

## Virusi informatici și antiviruși

**Virusul este un software, de regulă distructiv, proiectat pentru a infecta un sistem informatic.**

Virusii informatici sunt creați din diverse motive:

- un specialist vrea să-și demonstreze abilitățile
- o firmă producătoare de software își protejează programele (activează un virus la copierea ilicită)
- o firmă de soft producătoare de antiviruși lansează un virus pentru a-și vinde produsele.

Virusul prezintă **două caracteristici de bază: se auto-execută și se auto-multiplică.**

**Mecanismul de activare** verifică dacă s-a întâmplat un anumit eveniment sau o anumită condiție. Când aceasta are loc, virusul își execută obiectivul care de cele mai multe ori este unul nedorit, distructiv pentru sistemul informatic. În funcție de motivele autorului, **un virus poate crea daune imediat după execuția lui sau poate aștepta până când are loc un anumit eveniment.** În cazul în care **mecanismul de activare** verifică dacă a fost atinsă o anumită dată calendaristică pentru a executa virusul, putem spune că virusul este o bombă cu ceas (time bomb). Dacă se verifică existența unei condiții, ca de exemplu lansarea în execuție a unui program de un anumit număr de ori), putem numi **virusul bombă logică** (logic bomb). **Astfel pot exista diferite mecanisme de activare sau niciunul**, în acest caz existând doar infectarea inițială.

O dată ce virusul a fost activat, pot declanșa **acțiuni devastatoare** pentru un sistem cum ar fi:

- ștergerea informațiilor de pe sistemul de stocare
- schimbarea tabelii de partiții a hard disk-ului, care duce la imposibilitatea citirii informației de pe disc;
- distrugerea unor fișiere;
- modificarea dimensiunii fișierelor;
- ștergerea totală a informațiilor de pe disc, inclusiv formatarea acestuia;
- diverse efecte grafice/sonore inofensive;
- încetinirea vitezei de lucru a calculatorului până la blocarea acestuia.

Inițial virusul se află în interiorul unui program, strecurat printre instrucțiuni. Atât timp cât programul nu este executat, virusul nu este activat. Odată ce acesta a fost activat, virusul încearcă să se infiltreze printre instrucțiunile altor programe, contaminând întreg sistemul. Această acțiune poartă numele de mecanism de replicare.

**Mecanismul de replicare îndeplinește următoarele funcții:**

- caută alte programe pentru a le infecta;
- verifică programul găsit dacă a mai fost infectat anterior după semnătura virusului;
- inserează instrucțiuni ascunse în interiorul programului;
- modifică secvența de execuție a programului infectat astfel încât instrucțiunile ascunse să fie executate ori de câte ori programul este apelat;

- creează o semnătură pentru a indica faptul că programul a fost infectat pentru a nu fi infectat încă o dată .

Această semnătură a virusului este necesară pentru ca programele din interiorul sistemului informatic să nu fie infectate în mod repetat, acest lucru ducând la creșterea dimensiunii programelor și automat la detecția existenței virusului. Mecanismul de replicare poate îndeplini și alte funcții cum ar fi resetarea datei de modificare a documentului infectat la valoarea ei inițială (data la care a fost creat documentul) sau raportarea dimensiunii inițiale a documentului și nu pe cea în urma infectării.

**Virusii informatici pot fi clasificați în funcție de programul executabil în care se infiltrează sau în funcție de modalitatea lor de funcționare.**

**În funcție de programul executabil** în care se infiltrează, există mai multe tipuri de virusi:

- **virusi MBR** (Master Boot Record) – sunt acei virusi care infectează MBR-ul de pe hard disk-uri; MBR-ul fiind sectorul care conține un scurt program ce încarcă sistemul de operare. Dacă acest sector este corupt, sistemul de operare nu se mai poate încărca.
- **virusi BS** (Boot Sector) – sunt asemănători cu virusii MBR, singura diferență fiind că virusii BS au ca țintă dischetele, CD-urile sau DVD-urile;
- **virusi de fișiere** – sunt virusii ce infectează o anumită categorie de fișiere. De obicei sunt infectate fișierele executabilele (cele ce au extensia .EXE sau .COM), fișierele overlay (au extensia .OVL) sau fișierele de sistem (au extensia .SYS sau .DRV).
- **virusi de macro-uri** – virusii se plasează într-unul sau mai multe macro-uri din cadrul documentelor de tip Microsoft Office și utilizează funcționalitățile Visual Basic for Applications.
- **virusi pereche** – sunt virusii ce creează un fișier executabil nou, cu același nume, dar cu extensia .COM. Dacă sunt întâlnite două fișiere executabile cu același nume, dar cu extensii diferite: .COM și .EXE, sistemul de operare Microsoft Windows lansează întâi fișierul cu extensia .COM.
- **virusii de link-uri** – sunt virusii ce alterează structura de directoare, redirecționând calea directorului unui fișier infectat către zona în care este localizat virusul. După lansare, virusul poate încărca fișierul executabil, citind calea corectă a directorului fișierului respectiv.
- **virusi specifici** – sunt virusii ce infectează anumite aplicații:
  - **virusi de ActiveX** – sunt scriși pentru a infecta produsele Microsoft. Utilizează un cod încărcat pe un server și se răspândesc în stațiile locale;
  - **virusii VB script** – folosesc Visual Basic pentru a accesa un cod dăunător de pe un server web și a-l răspândi în stațiile de lucru locale. Este suficientă accesarea unei pagini web pentru a infecta sistemul local de operare;
  - **virusii de Java** – folosesc programele Java pentru a efectua operații nedorite pe stațiile de lucru.

**După modalitatea de funcționare și de tehnicile folosite**, virusii se clasifică în:

- **virusi invizibili** – folosesc tehnici de mascare care ascund faptul că sistemul a fost infectat. Când sistemul de operare încearcă să afle dimensiunea unui program infectat,

virusul ascuns scade o parte din aceste date, egală cu dimensiunea propriului cod și o înlocuiește cu datele corecte. Astfel, dacă programul este doar citit de un scanner de viruși, dar nu este rulat, codul viral este ascuns și nu poate fi detectat .

- **virusi polimorfici** – folosesc o tehnică de modificare a propriului cod viral, utilizând tehnici de criptare avansate. Acest proces de modificare se numește mutație. Prin mutație, un virus își poate schimba dimensiunea și compunerea. În plus, își pot modifica semnătura, fiind astfel mult mai greu de detectat de programele ANTIVIRUS.
- **virusi rezidenți sau non-rezidenți** în memoria calculatorului:
  - **virusi rezidenți în memorie** – se instalează la un nivel înalt la memoriei RAM pentru a se atașa fișierelor executabile sau documentelor de tip Microsoft Office ce sunt deschise la un moment dat. Acești viruși pot controla întregul sistem și îl pot infecta oricând.
  - **virusi non-rezidenți** – sunt activați numai la pornirea aplicației gazdă.

### **Măsuri de protecție împotriva virușilor**

- Verificarea datelor ce vor urma a fi introduse în calculator, cu un program antivirus.
- Evitarea folosirii unor soft-uri pirat (fără licență).
- Scanarea calculatorului cu un program antivirus.
- Păstrarea unor copii de siguranță ale aplicațiilor și fișierelor importante.

### **Programele antivirus**

Programele antivirus sunt create special pentru:

- detectarea virușilor prin verificarea conținutului fișierelor și semnalarea prezenței semnăturii unui virus cunoscut sau a unor secvențe suspecte în interiorul lor
- dezinfectarea sau ștergerea fișierelor infectate
- prevenirea infectării prin supravegherea acțiunilor din memorie și semnalarea întâlnirii unor anumite acțiuni care ar putea fi generate de existența în memorie a unui virus.

### **Programe antivirus - exemple:**

- Avira AntiVir Personal
- AVG Anti-Virus
- BitDefender Antivirus
- Kaspersky Anti-Virus
- McAfee VirusScan
- NOD32
- Norton AntiVirus
- Panda Antivirus
- Windows Live OneCare